Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems

verfassungsblog.de/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems-2/

Orla Lynskey Fr 9 Okt 2015

The *Schrems* judgment of the ECJ has implications for the viability of the commercial practices of Internet giants (and minions), for the legality of state surveillance practices and for the future sustainability of an Internet that is global rather than parochial. It is thus not surprising that the Court of Justice of the EU delivered its judgment only one week after the Opinion of the Advocate General and that this judgment has attracted so much academic and media attention, including through the existing commentary on this blog. In adding to this commentary, I shall not rehash the well-versed facts but shall focus on three points which I found striking.

Can any EU-US data transfer be compatible with the Charter at present?

In the aftermath of the *Schrems* judgment, some of the 5,000 or so companies which had self-certified under the Safe Harbour scheme, have been using alternative mechanisms foreseen by the Directive, such as Binding Corporate Rules (BCRs) and standard contractual clauses, to facilitate EU-US data transfers. However, it is difficult to see how these alternative transfer mechanisms could withhold judicial scrutiny. To focus on them is to overlook the underlying issue: the Court considered the general legal framework in the US to be lacking from a rights perspective. Once transferred to the US, the US legal framework allows for generalized access to this data by the National Security Agency. Moreover, it does not provide EU residents with any judicial redress, thereby infringing the essence of the Charter's right to effective judicial protection.

While these findings were made in the context of the Court's assessment of the validity of the Safe Harbour decision, the general US legal framework would be no more compatible with EU fundamental rights had the data transfers been reliant on another transfer mechanism. The Court held that US 'legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be recognized as compromising the essence of the right to respect for private life'. This leads to the inescapable conclusion that unless the US changes its rules on systematic communications interception, data transfers between the EU and the US will always breach the rights to data protection and privacy. This leaves companies reliant on data transfers in an unenviable position, with their most fruitful options being to either lobby for change of the US rules on communications interception or to restructure data processing operations, to avoid data transfers to the US.

Of course, the elephant in the room is the UK. The Irish High Court had relied upon documents made public via Snowden in reaching the conclusion, endorsed by the ECJ, that the US offered an inadequate level of protection to individuals. The Snowden revelations also demonstrate that the UK's Tempora programme was functioning in a similar manner to the US's Prism programme. EU countries enjoy a presumption of adequacy under the data protection rules. Moreover, the data protection regime allows for derogations for 'State security', amongst other interests. It would be interesting to consider whether the Charter's right to data protection would apply to the UK's intelligence and surveillance activities. The UK would undoubtedly argue that they benefit from an exemption to the data protection regime for state security purposes, however the Charter applies to Member States when 'implementing' EU law – including when derogating from EU law.

Rights over Market Integration

The Court, in line with its well-established *Foto-Frost* jurisprudence, affirms that only it has jurisdiction to declare that an EU act, such as the contested Safe Harbour decision, is invalid. The logic underpinning this exclusivity is to safeguard 'legal certainty by ensuring that EU law is applied uniformly' (para 61). However, the Court's late emphasis – also in line with its now-established case-law – on the complete independence of the national Data Protection Authorities (DPAs) is hard to reconcile with this insistence on legal certainty. The Court held that as

entities acting with ‘complete independence’, these DPAs should be able to examine all claims put before them and to exercise their powers pursuant to the Directive, including the power to suspend data flows. Overall, the Court’s finding in this regard is quite formalistic: it upholds its exclusive jurisdiction to annul an erroneous adequacy decision yet it allows 28 DPAs to suspend data flows if they consider the adequacy decision to be erroneous. There may therefore be uniformity on paper but not in practice, a recurring theme in the EU data protection law context. This is also another illustration of an emerging trend in the Court’s data protection case-law: fundamental rights concerns are allowed to trump market integration. This is not problematic per se but, once again, calls into question data protection’s origins as a legal instrument to promote market integration.

The Court’s concern (or lack thereof) for practical implications

The Court has been criticized extensively for overlooking the practical implications of its data protection jurisprudence. This was also a common theme in the aftermath of *Google Spain* and *Digital Rights Ireland* (where it refused to limit the temporal effects of its findings as the Advocate General had suggested). One concern, succinctly voiced by Kuner, is that it is unsustainable for the EU to impose very strict conditions on personal data processing in a pluralistic world with differing conceptions of rights: this may lead to the re-establishment of national or regional borders on the Internet. While this is a genuine concern, it is difficult to see how the Court could have held otherwise in this case in light of the established case-law of the European Court of Human Rights on communications interception and of its own jurisprudence in *Digital Rights Ireland*. If nothing else, it would have set up a primacy showdown with the Irish as the High Court judge had already indicated in his referring judgment that the data transfers from Ireland to the US violated Irish Constitutional rights. While one might suggest that the temporal effects of the Court’s finding could have been limited, given the protracted negotiations on a new Safe Harbour deal it is possible the Court felt that any such delay would simply be kicking a difficult ball into long grass.

There will be much deliberation in the coming months about how to route around the Court’s judgment: either the US changes its communications interceptions rules, or the EU changes its rules on adequacy in the final round of negotiations on the new General Data Protection Regulation. It is hard to predict who will blink first.

SUGGESTED CITATION Lynskey, Orla: *Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems, VerfBlog,* 2015/10/09, http://verfassungsblog.de/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems-2/.